الخليج

اقتصاد, تقنية وسيارات

11 يونيو 2023 16:53 مساء

أفكار خاطئة تحول دون تحقيق القيمة التامة للأمن السيبراني 4

سلّطت شركة «جارتنر» للأبحاث، الضوء على أربعة مفاهيم خاطئة تمثّل عقبة تحول دون تحقيق القيمة التامة للأمن السيبراني في قطاع المؤسسات، وتحد من فاعلية البرامج الأمنية. ودعت شركة الأبحاث المسؤولين التنفيذيين عن أمن المعلومات إلى اعتماد مبدأ «الحد الأدنى الفعّال»، بهدف تعزيز تأثير الأمن السيبراني على أعمالهم.

وقال هنريك تيكسيرا، كبير المحللين لدى «جارتنر»: «يشعر العديد من المسؤولين التنفيذيين عن أمن المعلومات بالإرهاق، ولا يعتقدون بأنهم قادرون على ضبط التوازن بين مسؤوليات العمل وحياتهم الشخصية. وعلى الرغم من أنهم يبذلون قصارى جهدهم، فإن قادة أمن المعلومات وفرقهم غير قادرين على تحقيق الأثر الأكبر».

- **75 % من الموظفين سيطورون تقنيات بعيداً عن تقنية المعلومات بحلول 2027**
- **69 % من الموظفين تجاوزا تعليمات الأمن السيبراني لدى مؤسساتهم خلال 12 شهراً الماضية**

• 74 % من الموظفين أبدوا الاستعداد لتجاوز التعليمات الأمن السيبراني فيما لو ساعدهم ذلك

وقال لي مكمولين، نائب الرئيس الأول للأبحاث لدى «جارتنر»: «يعد منهج الحد الأدنى الفعّال منهجاً مدروساً لإدارة الأمن السيبراني مستقبلاً بالاعتماد على عائدات هذه الاستثمارات، وعلى الرغم من أن فكرة «الحد الأدنى» قد لا تروق لسمع البعض، فإنها تشير إلى المُدخلات وليس إلى المخرجات، فهذه المنهجية تمكّن وظائف الأمن السيبراني من الوصول لما هو أبعد من مجرد «الدفاع عن الحصن» وإطلاق العنان للإمكانات الكامنة وتعزيز قيمتها الملموسة». وكشفت «جارتنر» عن أربعة أفكار خاطئة شائعة فيما يتعلق بالأمن السيبراني وفرص قادة أمن المعلومات لإضافة قيمة جديدة على مستوى مشاركة الأعمال، والتقنية، والكفاءات:

الفكرة الخاطئة الأولى: المزيد من البيانات يعني حماية أفضل

وبحسب «جارتنر»، يسود اعتقاد خاطئ أن الطريقة الأمثل لدفع اتخاذ إجراءات من قبل صنّاع القرار فيما يتعلّق بمبادرات الأمن السيبراني، هي من خلال تقديم تحليلات مركّبة للبيانات، مثل حساب احتمالية وقوع حدث أمني إلكتروني. لكن محاولة قياس المخاطر بهذه الطريقة لا تبدو خياراً عملياً. إضافة إلى ذلك، فإن هذه المنهجية لا تتيح مشاركة المسؤولية ما بين صنّاع القرار في المؤسسة وقادة الأمن السيبراني فيما يستدعي تقليل مخاطر الأعمال. وقد أشارت دراسة أجرتها «جارتنر» إلى أن ثُلث المسؤولين التنفيذيين عن أمن المعلومات ينجحون في تسجيل اتخاذ الإجراءات اللازمة من خلال تقديرات لحجم المخاطر الأمنية.

من أجل تطبيق نظرية الحد الأدنى (ODM) ويجب على قادة أمن المعلومات اعتماد منهجية مقاييس مدفوعة بالنتائج الفعّال؛ إذ تعمل هذه منهجيات على ربط المقاييس التشغيلية والأمنية بالنتائج الأعمال التي توفّر الدعم لها من خلال توضيح مستويات الحماية الحالية والمستويات البديلة المتاحة بناء على حجم الإنفاق المتوقّع.

الفكرة الخاطئة الثانية: المزيد من التقنية يعني حماية أفضل

تتوقع «جارتنر»، أن يسجل الإنفاق العالمي على خدمات ومنتجات أمن تقنية المعلومات وإدارة المخاطر نمواً بمعدّل 12.7% ليصل إلى قرابة 189.8 مليار دولار خلال عالم 2023. ولكن على الرغم من ارتفاع إنفاق المؤسسات على تقنية وأدوات الأمن السيبراني، فإن قادة أمن المعلومات لا يزالون يشعرون بعدم توفّر الحماية اللازمة.

وبإمكان المؤسسات أن تبدأ مشوارها نحو مجموعة أدوات «الحد الأدنى الفعّال» من منظور الكلفة البشرية، ولك من خلال الحرص على أن تبقى كلفة الإنفاق على المختصين بإدارة أدوات الأمن السيبراني أقل من مستوى الفائدة المرجوة من هذه الأدوات المستخدمة في الحد من المخاطر. وبالتوازي مع ذلك، اتباع منظور معياري لقياس ما إذا كانت إضافة توفير الدعم (CSMA) أو إزالة أداة ما قادرة على تعزيز الحماية للمؤسسة. كما أن بإمكان مبادئ شبكة الأمن السيبراني الأمني من خلال إتاحة التصاميم تدعم البساطة، والتوافقية، والعمل البيني.

الفكرة الخاطئة الثالثة: المزيد من مختصي الأمن السيبراني يعني حماية أفضل

يقول مكمولين: «يفوق الطلب على الكفاءات المختصة في الأمن السيبراني ما هو متاح في الأسواق إلى درجة أن قادة أمن المعلومات لم يعودوا قادرين على مواكبة الركب؛ إذ باتت الحماية تمثّل عنق زجاجة أمام التحوّل الرقمي، والسبب في ذلك يعود غالباً إلى الفكرة الخاطئة بأن المختصين بأمن المعلومات وحدهم قادرين على القيام بالمهام الجادة في تأمين الحماية السيبرانية. لكن الحل يبدو في تعميم الخبرات السيبرانية وإتاحتها للعموم بدلاً من السعي إلى تعيين هذه الكفاءات في ظل الفجوة الحالية في الأسواق».

وتتوقّع شركة «جارتنر» أنه وبحلول عام 2027، فإن 75% من الموظفين سوف يمتلكون، أو يطورون، أو ينشؤون تقنيات بعيداً عن تقنية المعلومات، أي بزيادة تصل إلى 41% مقارنة بعام 2022. وبإمكان قادة أمن المعلومات تخفيف الأعباء على فرق العمل لديهم من خلال مساعدة المختصين التقنيين لدى هذه المؤسسات في تطوير خبرات الحد الأدنى الفعّال، أو القدرة على اتخاذ الأحكام السيبرانية. فقد أشارت دراسة حديثة صادرة عن «جارتنر» أن قدرة الخبراء التقنيين المؤهلين على اتخاذ قرارات الأمن السيبراني لدى المؤسسات تتطور بمعدّل يصل إلى 2.5 مرة فيما يتعلّق بالتفكير في المخاطر السيبرانية، وذلك عند تطوير قدراتهم التقنية أو التحليلية.

الفكرة الخاطئة الرابعة: المزيد من الضوابط يعني حماية أفضل

كشفت دراسة صدرت مؤخراً عن شركة «جارتنر» أن 69% من الموظفين قد تجاوزا تعليمات الأمن السيبراني لدى مؤسساتهم خلال الأشهر الإثني عشر الماضية، وأن 74% من الموظفين أبدوا الاستعداد لتجاوز هذه التعليمات المتعلّقة بالأمن السيبراني فيما لو ساعدهم ذلك أو ساعد فرقهم في بلوغ الأهداف المنشودة للأعمال.

ويقول تيكسيرا: «تدرك مؤسسات الأمن السيبراني جيداً السلوك غير الآمن والسائد في أوساط القوى العاملة، إلا أن الاستجابة التقليدية المتمثلة في فرض المزيد من الضوابط تأتي بنتائج عكسية؛ إذ يُبلغ الموظفون عن مزيد من العراقيل التي تفرضها السلوكيات الآمنة، وهو ما يدفع إلى رواج بعض الممارسات غير الآمنة».